ABSTRACT

Described is a method and system for performing path-sensitive value flow analysis on a software program. Concrete state and value alias information is tracked along each statement and each relevant path in an abstract program and is stored as a symbolic state in a symbolic store. The value alias information includes a first set of aliases that identify aliases for a designated value that is being analyzed and a second set of aliases that identify possible aliases for the designated value. The value alias information is obtained using imprecise memory alias analysis. Along each relevant path for each statement, transforms are applied to the sets of aliases to update the first and second sets of aliases. The transforms are applied based on the type of statement being processed. Symbolic states existing at the same location are merged if the value alias information is identical within the symbolic states.